**Patent Claims**

1. A method for signing a message (22) by a sender (20), and for checking the signature by a receiver, wherein a control center (10) and a receiver (30) have a secret, common main key (11, 11'), having the following features:
   - the control center (10)
     * produces a sequence number (12) and
     * from this and using the main key (11) produces a signing key (14) by means of one-time encryption (13), and
     * provides the sender with the signing key (14);
   - the sender (20)
     * uses the signing key (14) to form a signature (22c) for the message (21, 22c) and
     * sends to the receiver a message set (22) which contains at least the message (22b) and the signature (22c).
   - The receiver (30)
     * determines the sequence number (22a'),
     * forms the one check key (14') using the one-time encryption (13') and the main key (11'), and
     * uses this to check the signature (22c) on the message.

2. The method as claimed in claim 1, wherein the sequence number (12, 22a, 22a') is transmitted together with the signing key (14) from

the control center to the sender (20), and is transmitted from the sender (20) via the data set (22, 22') to the receiver.

3. The method as claimed in claim 1, wherein the sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the receiver.

4. The method as claimed in claim 1, wherein the sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the sender, and is transmitted via the data set (22, 22') to the receiver.

SUBA2 5. The method as claimed in one of the preceding claims, wherein the sequence number is produced by a pseudo-random number generator.

6. The method as claimed in one of the preceding claims, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.

7. The method as claimed in one of the preceding claims, wherein the control center (10) produces a number of signing keys (14) in advance, and transmits them to the sender (30), possibly together with the associated sequence numbers (12).

8. The method as claimed in one of the preceding claims, wherein the receiver (30) maintains a list of already used sequence numbers, and rejects already used sequence numbers.

9. A device for signing a message (22, 22') which is sent from a sender (20) to a receiver (30), having the following features:

- a control center (10) and the receiver (30) have a first and a second memory for a secret, common main key (11, 11');
- in the control center (10), one input of a first one-time encrypter (13) is connected to the first protected memory (11), and another input is connected to a generator (12) for a sequence number,
- the output of the one-time encrypter (13) is connected to the sender (20) via a transport medium,
- a signature generator (24) is provided in the sender, and its inputs are connected to the output of the one-time encrypter and to the message (21, 22b) to be signed,
- the output of the signature generator (24) is connected to a device which assembles at least the signature (22c) and the message (22b) to form a message block (22) and whose output is connected to the receiver (30) via a transport medium,
- a signature checker (22') is provided in the receiver, whose inputs are connected firstly to the message (22b') and to the signature (22c) of the message block (22') which has arrived via the transport medium,
- and secondly to the output of a second one-time encrypter (13'), whose inputs are connected firstly to the second memory (11') for the

secret main key and to a means for providing a sequence number (22a').

SUBA37

10. The device as claimed in claim 9, wherein a generator produces the sequence number (22a') using a deterministic method, [lacuna] one or more sequence numbers corresponding to the number of checks.